December 5, 2010

By electronic mail

Secretary S. Kimberly Belshé
California Health and Human Services Agency
1600 Ninth Street, Room 460
Sacramento, California 95814

Mr. William Barcellona
Co-Chair, California Privacy and Security Advisory Board
c/o California Association of Physician Groups
1215 K Street, Suite 1915
Sacramento, California 95814

Ms. Pamela Dixon
Co-Chair, California Privacy and Security Advisory Board
c/o World Privacy Forum
2033 San Elijo Avenue, No. 402
Cardiff by the Sea, California 92007

RE: THE CALIFORNIA PRIVACY AND SECURITY ADVISORY BOARD'S MEETING TO RECONSIDER ITS RECOMMENDATION REGARDING PATIENT CONSENT ON OCTOBER 12, 2010

Dear Secretary Belshé, Mr. Barcellona, and Ms. Dixon:

Consumers Union and Center for Democracy & Technology provide the following materials in response to the California Privacy and Security Advisory Board's invitation and subsequent questions forwarded by electronic mail from Ms. Bobbie Holm on November 9 and December 2, 2010.

Question 1: Please provide the legal basis for supporting the Tiger Team proposal considering California's constitution and law.

Our letter requesting reconsideration, dated October 26, 2010, already summarizes that California law does not require an opt-in patient consent policy across the board for electronic health information exchange, while it does require the patient's prior consent

West Coast Office
1535 Mission Street
San Francisco, CA 94103
415.431.6747 tel
415.431.0906 fax
www.consumersunion.org

for disclosures of specific categories of information such as HIV test results and psychiatric records. We attach a copy of that letter for your convenience. We note that various officials at the California Health and Human Services Agency have agreed in subsequent conversations that California law does not require across the board an opt-in patient consent policy for electronic health information exchange.

Question 2: Please provide substitute guideline language that would represent the Tiger Team proposal.

We attach a proposed alternative to Guideline 2.1 on patient consent. We explain the core amendments below, but the attached draft includes additional, conforming amendments as needed.

We were constrained by the fact that Guideline 2.1 concerns patient consent only, while the Tiger Team's recommendations appropriately consider patient consent in the context of fair information practices collectively. Amending Guideline 2.1 only misses an important threshold opportunity to advance a patient-centered health care system by adopting a comprehensive framework of fair information practices and privacy and security protections such as that recommended by the Tiger Team.[1] We urge CalPSAB to incorporate a more complete set of fair information practices into the Guidelines before they are finalized.[2]

Given the constraints above and the limited time available for reconsideration, we also attempted to minimize the amount of revision to Guideline 2.1 as recommended on October 12, 2010. The simplest approach, we believe, is amending the definition of electronic health information exchange so that it is limited only to those uses of an electronic health information exchange that require meaningful patient consent under the Tiger Team's recommendations. This requires amending the definition of Electronic

[1] The Tiger Team's recommended framework is rooted in the widely accepted Fair Information Practices (FIPs), a set of policies for privacy and security that form the basis for many laws in the United States and internationally. The Fair Information Practices include transparency about data policies; limiting the collection, use, and disclosure of health information to what is necessary for the particular purpose; protecting the quality, integrity, and security of the information collected; and ensuring accountability through appropriate audit trails and enforcement. These principles operate in tandem with one another; overreliance on one or some principles weakens the greater collective effectiveness of the fair information practices, but utilizing the whole set maximizes comprehensive privacy and security protection. The Tiger Team's approach applies these fair information practices to electronic HIE.

[2] To the best of our knowledge, based upon a review of the archives for CalPSAB on the website, the Advisory Board has only voted on a fraction of the Interim Guidelines, and those votes addressed underlying policy or principle and did not approve particular language in particular guidelines.

Health Information Exchange in the Interim Guideline's definitions; amending Guideline 2.1 to require opt-in consent when an Electronic Health Information Exchange is not used for directed exchange among providers for purposes of diagnosis, treatment, care coordination, or public health reporting; and amending Guideline 2.1 to require that, when patient consent is required, it should be meaningful in accordance with the Tiger Team's recommendations.

a. Definition of "Electronic Health Information Exchange (eHIE)"

Accordingly, we propose the following definition of "electronic health information exchange":

> Electronic Health Information Exchange (eHIE): A formal electronic health information exchange infrastructure formed to facilitate the exchange of electronic health information among unrelated or unaffiliated healthcare entities for treatment, care coordination, and other agreed-upon health care purposes.* An eHIE is characterized by agreement among participants to allow one another to have access to identifiable health information from clinical records in accordance with common terms of participation.

This definition also clarifies that "electronic health information exchange" in Guideline 2.1 and throughout the Interim Guidelines refers only to use of a formal electronic health information network, and does not instead embrace all electronic exchange of health information irrespective of the mode of exchange. Not only is this amendment necessary to comport with the Tiger Team's recommendations, but we note the perverse outcomes that could occur if the Guidelines covered any electronic exchange of data, whether through an HIE/HIO network or point to point between two discrete entities. Unless and until the patient opted in, entities which today may share data electronically for diagnosis, clinical treatment, and care coordination would have to share these data in paper form for any of those purposes. This does not advance meaningful use by patient or provider. Such constraints instead create incentives for providers not to adopt electronic health records, and those providers who chose to move forward with health information technology would still have to maintain a duplicate paper record in order to accommodate every patient who had not opted in, for as long as they have not opted in, in order to share health information with doctors, hospitals, pharmacies, and laboratories for purposes of treatment and care coordination.

---

* Organized Health Care Arrangements, as defined in the HIPAA Privacy Rule, and exchange among entities that share a corporate relationship or affiliation and therefore a common patient record should not be considered eHIEs for purposes of treatment, care coordination, and public health and quality reporting, per the Tiger Team's recommendations. The patient has prior notice and expectation of such joint arrangements as required by the Privacy Rule.

b. Requiring Opt-In Consent for Exchange via an eHIE

In some models of an electronic exchange, a provider may continue to control the decision to disclose information from the patient's record, just as a provider in directed exchange (e.g. one provider directly to another) currently controls the decision to disclose information and the kind and volume of information to be shared with others providing treatment to the patient. In such models, for example, this control may be retained under the provider's agreements with the electronic health information exchange, or under the electronic health information exchange's own standards.

In other agreements or models of an exchange, however, the provider may no longer have control over decisions to disclose information from the patient's record. The Tiger Team recommended that meaningful patient consent (whether opt in or opt out) should be required when the provider no longer has control over decisions to disclose the patient's information to others or when or how clinical records are accessed. Thus, for example, meaningful patient consent would be required for exchange models involving centralized databases, where physicians or others can query and obtain information about a patient based solely upon the terms of participation in the exchange and without an intervening judgment or prior decision to disclose by the provider or entity which created and is responsible for the patient's record.

To implement these Tiger Team's recommendations, therefore, we propose the following amendment to Guideline 2.1 specifying when opt-in consent is required:

> Where, under the terms of participation in the eHIE or the entity's agreement with the eHIE, an entity would no longer control the decision to disclose a patient's information or the kind or volume of information to be disclosed, or where consent is otherwise required by federal or state law, ~~N~~no individual health information shall be exchanged via the eHIE except as required by law if the entity does not obtain or verify an individual's meaningful consent through the procedure described below.

As we explained in our briefing paper, this tracks patient expectations regarding the confidentiality of their data and the judgment of providers to use that data to render effective treatment.

c. Requirement of Meaningful Consent

Under the Tiger Team's recommendations, where consent is required the patient's consent must be meaningful. The patient should have knowledge and time in advance to make the decision whether to consent—for example, outside of the urgent need for care. Consent should not be compelled or used for discriminatory purposes—for example, consent to participate in a centralized HIO model or a federated HIO model should not be a pre-condition of receiving necessary medical services. The request for consent should include full transparency and education: the patient should receive a clear explanation of the choice and its consequences, in consumer-friendly language that is conspicuous at the

time of decision. The request for consent must be commensurate with the circumstances. For example, the more sensitive or inscrutable the activity, the more specific the consent mechanism should be; and activities that depart significantly from reasonable patient expectations require greater degrees of education, time to make the decision, opportunity to discuss the question with the provider, etc. The request for consent must be consistent with reasonable patient expectations for privacy, health, and safety. Lastly, the patient must be able to change consent preferences at any time and revoke consent altogether, and the consent request should clearly explain whether such changes can apply retroactively to data copies already exchanged, or whether they only apply prospectively from the time of change.

Some of the Tiger Team's recommendations for meaningful consent already exist more or less in Guideline 2.1. Some elements of meaningful consent, however, are missing. Accordingly, we propose the following amendment to Guideline 2.1.6, adding Guideline 2.1.6.2 on "Meaningful Consent":

To ensure that the consent is meaningful, an entity shall:

- Allow the individual advance knowledge and time to make the decision on consent, e.g. outside of the urgent need for care.
- Not compel or use the consent for discriminatory purposes, e.g. condition receiving necessary medical services upon consenting to participation in an eHIE.
- Provide full transparency and education, so that the individual receives a clear explanation of the choice and its consequences, in consumer-friendly language that is conspicuous at the time of decision.[3]
- Make the explanation and process commensurate with the circumstances, so that information or exchange that is more sensitive or inscrutable receives a more specific consent mechanism, and activities that depart significantly from reasonable patient expectations trigger a greater degree of patient education, time to make the consent decision, opportunity to discuss the decision with the provider, etc.
- Make the consent process consistent with reasonable patient expectations for health, privacy, and safety.
- Make the consent revocable at any time and explain the rights and terms of revocation under 2.1.7 Revocation of HIEconsent Decision and 2.1.8 Applicability of a Revocation.

[3] We note that this provision overlaps with current Guideline 2.1.6 Informing Individuals of HIEconsent and 2.1.6.1 General Informing Requirements, but it still warrants inclusion here as a necessary component of "meaningful consent."

Question 3: Please address how do you reconcile the current inadequacy of most EHR technologies to segregate sensitive data from exchange and your proposal.

Segregation of sensitive data is not a legal requirement; segregation is instead a technological tool that can assist providers in complying with additional privacy requirements (such as consent) on particular types or categories of data. The fact that this technological approach is not yet mature or widespread in electronic health records does not mean that other methods of honoring patient preferences and better policies regarding patient consent are not available. The Tiger Team's approach builds upon the current legal requirements and the approaches providers successfully implement today.

California's providers today must obtain a patient's consent before disclosing certain types of health information, regardless of the medium in which that information is held. That is clear policy. Where a particular document or record contains both information requiring specific consent before it may be shared and information that does not, the provider must obtain the patient's consent to disclose the information requiring specific consent. If the patient does not consent, the provider either must redact or may not disclose the record. Redaction is likely common for paper records. If electronic records cannot excise the sensitive information, the provider must print the record and disclose it without the sensitive information. This is likely how providers handle the issue today. As another (albeit less desirable) option, providers can decide to keep more sensitive information out of the electronic record to avoid inadvertently disclosing it without patient authorization.

Moreover, we believe that requiring a blanket opt-in consent for all subsequent electronic exchange of sensitive information (current Guidelines 2.1 and 2.1.6.1(k)) is inconsistent with California law, while the Tiger Team's approach facilitates compliance with California law because it rejects a one-size-fits-all approach. California law requires the patient's consent before certain types of sensitive information may be shared, such as HIV test results and mental health records.[4] For example, California law requires specific written authorization prior to disclosing the results of an HIV test. Consent "is required for each separate disclosure of the test results, and shall include to whom the disclosure would be made."[5] The Confidentiality of Medical Information Act mandates different requirements prior to disclosing a patient's information relating to treatment with a psychotherapist, including notice of "the specific information," "its specific intended use or uses," the "length of time during which the information will be kept before being destroyed or disposed of," etc.[6] One blanket opt-in consent in advance for all subsequent electronic exchange of all categories of sensitive information does not meet these distinct requirements.

---

[4] See, e.g., Cal. Civil Code § 56.104; Cal. Health & Safety Code § 120980.

[5] Cal. Health & Safety Code § 120980.

[6] Cal. Civil Code § 56.104.

The Tiger Team's approach maintains the disclosing provider's obligation to comply with these specific laws by whatever means are necessary—whether by technology, where such tools are available, or by well-established approaches used today. Such particularized consideration and notice by the provider and consent by the patient before each special disclosure is also far more "meaningful" than one blanket consent in advance for all categories of sensitive information known and unknown.

As a final point, the preamble to Guideline 2.1 lists five strategies for safeguarding individual health information and notes that "technological limitations may not currently allow for the implementation of all of the above safeguards." The preamble does not list consent as a safeguard for individual health information, but rather presents consent as a way to educate the patient to understand and consent (or not) to the failure to have proper safeguards. Guideline 2.1 now requires prior ("opt-in") consent to any exchange because sensitive health information might be shared as well, and Guideline 2.1.6.1 explicitly requires informing the patient that "the individual's sensitive health information may be exchanged which might include references to HIV status, alcohol and drug abuse treatment records, mental health records, genetic information, and other potentially sensitive information." We have already explained why we think such a policy does not comply with California law. But such a policy also excuses providers and EHR vendors from implementing strong privacy policies and effective technological safeguards and instead shifts the burden to the patient. The Tiger Team's approach instead considers patient consent in the context of fair information practices collectively rather than shift the burdens and risks to patients.

Question 4: Please address if your proposal would result in different consent standards existing simultaneously in California, one for those who could meet all the security and segregation of data requirements and those that cannot.

As a threshold point, we note that California law already has multiple consent standards, as we explain above, and California law does not require segregation of data per se, as we also explain above. Current Guideline 2.1 actually exacerbates this circumstance by requiring a new, special consent obligation for EHR users that does not apply to exchange of the same information by fax, mail or telephone.

Unlike current Guideline 2.1, the Tiger Team's approach does ***not*** add a new opt-in consent standard where directed exchange via an eHIE occurs, but instead incorporates and builds upon existing law, practice, and technical capabilities, for reasons we explained at length in our briefing paper. But in exchange models where the provider no longer controls the decision about who can access the patient's information from her or his medical records, and what types and amounts of information are accessed, the situation is significantly different and a different consent standard is warranted.

Unlike current Guideline 2.1, the Tiger Team's approach also does not add a new consent standard for all electronic exchange, whether by eHIE or otherwise. We have not done a nation-wide survey of other state HIE policies, but according to the best evidence

that we have, states that are building formal electronic health information infrastructures have developed consent policies that apply solely to information included in or shared through that infrastructure, and rely on their existing laws to cover exchange outside an eHIE.[7]

Conclusion

California rightly calls electronic health information exchange (HIE) a cornerstone of health care reform in this state. Unless patient consent policy ensures that patient data flows smoothly and securely for core activities such as clinical treatment without repeated halts for permission, then California's HIE network risks impeding rather than facilitating electronic health information exchange in California. The Tiger Team's framework for privacy, security, and patient consent is well-vetted, incorporates and builds upon existing law and structures, and minimizes the need to invent new systems and policies with new trainings. It thus facilitates early adoption of electronic health records, especially by smaller providers more concerned about unfamiliar systems and procedures. This in turn promotes the meaningful use necessary to improve Californians' health and health care, maximizes California's entitlement to incentive payments, and reduces costs.

We note that the Tiger Team's recommendations are limited to Stage 1 of meaningful use, which is focused on sharing information between providers. More work must be done to develop privacy protections for the range of disclosures and uses of health information, including shoring up protections for de-identified data. This does not make the Tiger Team's recommendation irrelevant, however, because the Guidelines already limit electronic exchange to the same types of data sharing required for Stage 1 of meaningful use. In addition, the Tiger Team's approach, grounded in the fair information practices, provides a strong foundation for developing additional policy for Stage 2 and Stage 3 of meaningful use and other authorized uses and disclosures; but like the Tiger Team, we limit our proposed alternative to this initial stage with use of the electronic health information exchange limited to diagnosis, treatment, care coordination, and

[7] Melissa Goldstein & Alison Rein, "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis" (Mar. 23, 2010) (study prepared for Office of Policy and Planning, Office of the National Coordinator for Health IT) (available at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1147&parentname=CommunityPage&parentid=32&mode=2&in_hi_userid+11113&cached=true); New York Statewide Collaboration Process & New York Health Information Security and Privacy Collaboration, "Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York to Advance Interoperable Health Information Exchange to Improve Care" (Nov. 25, 2008) (available at http://www.nyehealth.org/images/files/File_Repository16/pdf/Consent_White_Paper_20081125.pdf).

public health reporting under the Advisory Board's recommended framework adopted on September 16, 2009.

In addition, we have limited ourselves to the issue under reconsideration, patient consent, and thus have not included recommendations we might make on any other issues.

We very much appreciate your consideration of these recommendations and look forward to discussing with the Advisory Board on December 9, 2010, how they could provide a sound approach to patient consent policy for electronic health information exchange in California. If you have any questions or thoughts before then, you can reach us through Mark Savage at (415) 431-6747.

Respectfully,

Mark Savage
Consumers Union of
United States

Deven McGraw
Center for Democracy
and Technology

enclosures:

1. Center for Democracy & Technology and Consumers Union, Briefing Paper: A Sound Approach to Patient Consent, Privacy, and Security for Electronic Health Information in California (Oct. 6, 2010).
2. Letter from Mark Savage and Deven McGraw to Secretary Kim Belshé, William Barcellona and Pamela Dixon (Oct. 26, 2010).
3. Proposed Alternative Guideline 2.1 (amending version adopted Oct. 12, 2010).

cc: Jonah Frohlich, Deputy Secretary, Health Information Technology
Alex Kam, Acting Director, Office of Health Information Integrity
Bobbie Holm, Policy Branch, Office of Health Information Integrity